PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Brian William HOLMES	Group Art Unit: 2872
Application No.: 10/585,189	Examiner: J. CALLAWAY
Filed: October 30, 2006	Docket No.: 128605

For: SECURITY DEVICE USING PARALLAX MOVEMENT TO VIEW FRONT AND REAR LAYERS

DECLARATION UNDER 37 C.F.R. §1.132

I, Brian William Holmes, a British citizen of Gnomes Oak, Fleet, Hampshire, GU51 5HZ, United Kingdom, do hereby declare as follows:

1. I am the sole inventor of the invention described and claimed in U.S. Patent Application No. 10/585189, filed on 30 October 2006.

2. I have a doctorate and have been working in the design and construction of holograms for over 20 years.

3. I am very familiar with the patent application, having refamiliarized with the specific disclosed details in reviewing the Office Action dated October 2, 2009, and U.S. Patent No. 4,568,141 to Antes (hereinafter "Antes"). I comment below on the relationship between the device disclosed in Antes and my invention.

4. Antes is recognized as the primary patent obtained by Landis & Gyr to protect their Kinegram™ technology.

5. The device described in Antes is an embossed security device comprising a complex arrangement, or pattern, of diffraction gratings. Typically, a visible image is generated by arranging the gratings in an ensemble of curvilinear tracks, or line structures, such that when

the device is rotated about an axis normal to its surface plane, specific tracks and grating elements will diffract into the observer's eye in a progressive and continuous manner to create an effect of a continuously transforming image (the dynamic or kinetic color pattern) - elements of which are visible at all angles within an angular viewing hemisphere. From an origination perspective, the proprietary Kinegram™ diffraction grating recording system is analogous to a line plotter that builds up the image by writing line patterns that continuously transform into neighbouring elements, *i.e.*, the pen of line plotter is generally not raised when progressing from one curvilinear line pattern to the next.

6. Considering Figure 1 of the Antes patent, this Figure shows an elementary example of the claimed device in which the color pattern 10, *i.e.*, the dynamic diffractive image, is provided by linear tracks Bi - though as Antes says in column 4, lines 1-5, the tracks may be also circular, annular or irregular, which is best summarized as curvilinear .

7. Dynamic movement of color is provided within each track Bi by dividing into a series of structural elements Sn, shown in Figure 1, and more explicitly in Figure 2. Each structural element Sn is distinct from neighbouring elements by virtue of its grating characteristics - that is a grating pitch or constant and a grating orientation φ (see column 5, lines 47-68, and column 7, lines 1-44) .

8. To understand the role of grating pitch and orientation, I first refer to Figure 3 of Antes, which shows the angular hemisphere of incidence and diffraction angle. Antes also provides three axes - the z axis which is normal to the plane of the device and the x and y axis. Imagine a light ray of a particular wavelength incident on a particular structure element of the device traveling along a z-axis. The angle by which that ray is diffracted back toward an observer relative to the z-axis will be determined by the grating pitch or constant, and reflective to the y-axis will be determined by the azimuth angle φ. Strictly speaking, this

angle is the angle made by the diffracted ray's projection onto an x-y plane. It should be noted light is always diffracted in a direction orthogonal to the grating pitch.

9. Finally, for an optical security device, the incident light is white or polychromatic. When white light hits a particular structure, the effect of diffraction will be to disperse it into a spectrum of colors forming a different angle with the z-axis according to the diffraction equation $\sin \theta = d/\lambda$.

10. Antes notes, for example, at column 5, lines 47-68, that, if a structural element has a grating pitch = 0.7µm, it will diffract or disperse white light in an angular band from 35 degrees to 90 degrees relative to the z-axis, e.g., deep red colors approaching 90 degrees and deep blue approaching 35 degrees. A structural element of grating pitch = 1.2 µm will diffract light in a band from 19 to 35 degrees. If the grating pitch = 2.2 µm, it will diffract the light in an angular band from 10 degrees to 19 degrees. Antes summarizes this in Figure 4 where the reference shows the hemisphere of angular diffraction pertaining to these three grating values, *i.e.*, the reference splits the hemisphere into three functional bands or rings covering the dispersion angles 10-19°, 19-35° and 35-90° pertaining to the three grating pitches.

11. It should be clear that these dispersion bands or rings do <u>not</u> represent discrete image planes distributed along the z-axis, which might be appropriately considered as representing planes of depth. Rather, the dispersion bands or rings represent viewing zones but these are strictly angular viewing zones, *i.e.*, angles to look along to see the desired optical effect.

12. In summary, Antes teaches how to construct a dynamic two-dimensional light pattern or image by the predetermined arrangement of elementary diffraction gratings (the structure elements). Indeed the Kinegram™ security device (which is described by the Antes patent) is marketed as a two-dimensional optically variable graphics feature which both technically and

visually is complementary to conventional security holograms and their multi-layered image effects.

13. Antes, therefore, does not relate to the relationship between depth and parallax movement. Accordingly, Antes fails to teach, and would not have rendered obvious, a first holographic image element in an image plane spaced from the surface of the microstructure, the device exhibiting at least one further image in a plane spaced from said image plane of the first holographic element, as claimed in claim 1.

14. Because the dispersion bands or rings in Antes represent viewing windows or zones, Antes would have only suggested particular viewpoints to one of ordinary skill in the art, and not anything relating to the spacing between holographic elements.

15. Lastly, Antes is directed to a 2D arrangement of diffraction gratings. There is nothing in Antes to suggest the claimed layer imagery.

16. For reference, I attach a copy of Chapters 9 and 11 (pages 169-185;207-225) from the textbook "Optical Document Security," edited by Rudolph L van Renesse and published in 1994 by Artech House Inc. Chapter 9 is by Dr. Moser, the Head of the Advanced Research Division at Landis & Gyr (the Assignee of the Antes patent), and describes the Antes device in considerable detail. As explained in lines 9-13, page 177, the Antes device is known as a Kinegram® and is referred to on page 177 of the textbook as reference 13. The textbook explains, beginning at page 177, line 3, that the Kinegram® exhibits a number of kinematic effects when it is rotated, such as translation, rotation, centrifugal or centripetal radial movement, expansion, contraction, and staggering towards background or foreground. However, there is no indication that the Kinegram® forms images out of the plane of the device. Thus the Antes device is a 2-D device.

17. The textbook, on page 212 in Section 11.3.1, lines 6-13, discusses the history of Kinegrams® and asserts that their advantage is that they are 2-D and not 3-D devices. This

explanation is further explained with reference to Figure 11.2 (page 215) which is almost identical with Figure 4 of the Antes patent. Figure 11.2 is describing the various viewing zones for observing the Kinegram® and is certainly not suggesting that images are formed in any planes other than the plane of the device itself.

18. As indicated above, Antes, therefore, does not relate to the relationship between depth and parallax movement. Further, Antes is merely directed to a 2D device. Accordingly, Antes fails to teach, and would not have rendered obvious, a first holographic image element in an image plane spaced from the surface of the microstructure, the device exhibiting at least one further image in a plane spaced from said image plane of the first holographic element, as claimed in claim 1.

I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine and/or imprisonment under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing therefrom.

Date: 28/06/2010

Brian Holmes
BRIAN WILLIAM HOLMES

Chapter 9

Document Protection by Optically Variable Graphics (Kinegram)

J.-F. Moser

9.1 INTRODUCTORY REMARK

The author of this chapter always defended and still defends the basic argument that technical descriptions of security technologies should in no case be made available to the general public. It is still a part of a strictly practiced philosophy within Landis & Gyr that the addressees of such information must be proven institutions and organizations combating fraud and counterfeit as their basic activity. This explains why Landis & Gyr's optically variable graphics (OVG) and, specifically, kinegram technology has up to now very rarely been a part of a written or spoken contribution to security conferences, where attending specialists have not been checked thoroughly on their preregistered identity.

The author is therefore aware of the risk in participating as a contributor to this book, which contains a condensation of the many optical techniques to protect documents against fraud. In full compatibility with the security philosophy developed at Landis & Gyr, as a long-time provider of substitute money, banknote acceptor, and passport and banknote security solutions, this contribution is restricted to matters enabling the general public, for their own protection, to make an easy and most effective use of the Landis & Gyr optical technology. It contains information that is and can be disclosed to the press.

For the sake of completeness, interested professionals and users of the Landis & Gyr technology are referred to the high security release procedures in use at Landis & Gyr. These provide all the information necessary to implement and use the technology for any application.

9.2 INTRODUCTION AND HISTORICAL BACKGROUND

The first systematic analysis of the possible impacts of laser optics on Landis & Gyr future products started in 1971. In 1972, Landis & Gyr launched a new research and development program on modern optics, which at that time referred to emerging laser physics and its applications, including holography. The program aimed at coding, reading, checking, and assessing authenticity, as well as at the development and recognition of cost-efficient and secure authenticity marks for the purpose of identification and authentication of persons, payment means, and documents.

The first concrete target was the development of a prepaid card based on optical technology and used for telephony applications. In 1973, the card concept and the principles of reading and irreversible erasing of the optical information were defined. This involved diffraction optics as basic optical technique applied under extremely severe security conditions: the information is invisibly anchored in the card, interrogated in the reader by optical reflection from one side, irreversibly, and irrecuperably destroyed from the other side while the change of the optical information from the initial to the final state is controlled. Today's card still works on that principle.

The second target was the development of new optical, cost-efficient, and small-scale techniques for automatic authentication of banknotes, to be integrated in vending machines operated by the general public. Banknote acceptors were already sold by Landis & Gyr in 1968, but the machine was a relatively bulky stand-alone instrument with too many complicated authentication tests. The new tests envisaged were subdivided in a category aiming at the authentication of banknotes not prepared for automatic testing (passive tests) and a category for banknotes specifically prepared to be read by machine (active tests). In the latter case, the activity necessarily involved the development of high-security machine readable *marks* to be integrated in the banknote. The overall activity demanded a strong and close cooperation with banknote and banknote paper makers and the banknote issuing authorities.

In early 1975, a first functional model of a prepaid card and card reader was available. It worked with an optical information track that contained an array of rectangular areas coded by a process that used holographic techniques. In 1976, after critical analysis of the technical performance, release was given to begin producing prepaid cards and corresponding readers on factory level. Also in 1976, the first holograms were applied on Swiss banknotes on a trial level. The in-plane focused phase holograms, which were embossed into special pigmented thermoplastic intaglio inks printed on paper, showed easily recognizable images (see also Chapter 8, Section 8.4.3). Unfortunately, they did not stand up to the rigorous standard durability tests practiced by banknote makers. This was mainly due to the fact that the holographic profiles had to be left uncovered to yield a sufficient visibility and that even the softest crumpling of the banknote paper carrying the hologram destroyed its image.

Particular milestones were marked in 1979 and 1980 [1]. The Swiss National Bank ordered a large-scale development project to be followed by an industrialization

phase to secure Swiss banknotes by holographically made machine-readable optical codes. The notes had to be read by centralized banknote checking machines at speeds of up to 20 notes per second. In March 1979, the first prepaid Phonocard® system with optically coded cards and readers was inaugurated in Brussels. The term *optically coded cards* refers to the fact that the former holographically coded track had been replaced by a far superior optical diffraction code technology that offered security against fraud far beyond what holography could do. This had become necessary because our own lab trials of even the best secured holograms had shown insufficient resistance against counterfeiting.

At the request of the Swiss National Bank, we organized the 1981 International Symposium in Lucerne, where we presented the state of the art of the new technology to a selected group of banknote paper manufacturers, printers, and issuing authorities [9]. The attendance and the overwhelming interest was remarkable. Among the 30 experts, the feeling was that not only machine-readable devices were necessary but, in particular, a once-and-forever increase of visual and machine recognition security.

While the telephone card interest marked a steady growth, optically variable plain color flips were developed for banknote and card applications. Despite the visual attraction of the color flips, we decided in 1982, very shortly after the first trials, to abandon this type of diffraction OVD. Human unreliability in secure color recognition, source dependence, and evident lack of security made this type of security device highly questionable (Section 9.4.2). Instead, we decided to embark on new features based on "living" images with predictable image movements that were to be color independent. The optokinematic (OK) feature was born (Figure 9.1) (see Appendix A). It immediately attracted intensive interest worldwide. In 1983, we presented the product at the Bureau of Engraving and Printing (BEP) in Washington. In 1984, further improvements and refinements lead to the first consolidated product, which we named *kinegram*.® The development and supply of kinegrams is restricted to applications on security documents. The term *kinegram* is protected as a trademark by Landis & Gyr Corporation. Jointly with De la Rue Giori SA, the world's largest provider of banknote manufacturing equipment, we responded positively to a request from the BEP. However, the high kinegram technology did not outweigh the costs involved, which at that time were certainly a major factor.

In October 1983, we produced prepaid cards at a rate of 500,000 cards per month and, in May 1984, 10 million cards had been sold. In addition, readers for prepaid tokens for vending electricity and gas were launched in early 1984. The project with the Swiss National Bank was concluded with a technical success. An industrial quantity of notes had received the machine-readable optical mark. The technology consisted of embossing the optical code directly on banknote paper fields covered with a special thin foil and the subsequent protection of the microstructure with a thin coat. Our high-speed reading equipment, developed for this mark, worked well at speeds of up to 20 notes per second. To restrict development costs a two-color MAN offset press was reinstalled to perform the embossing process. This certainly was a major reason

for not quite reaching the targeted low waste and scrap levels. It would be interesting to pursue the technology in the view of today's expertise.

The systematic introduction of the kinegram into the market started in 1985. This product is now protecting Austrian and Finnish banknotes; Saudi Arabia, the United States, Singapore, and Brunei passports; German, Benelux, Singapore, and Schengen visa stickers; Italian police, Netherlands ID cards. Furthermore, the Swiss National Bank has decided to secure all future currency denominations with kinegram elements starting in 1995 [2]. In the meantime, various papers on the subject have been presented at conferences on banknotes [3,4,8,9]. Within ISO 9000—quality procedures, a stringent quality system for OVG security elements has been introduced, encompassing the complete process chain from first contacts with the client to the last delivery of the product, including production operation, training, and servicing.

Also since 1985, the Landis & Gyr optical card market grew steadily, reaching, cumulatively, 100 million cards in December 1988 and 300 million cards in May 1992. Today, the world Landis & Gyr production capacity has nearly reached 100 million cards per year and is still expanding. A newly developed production process chain is being started at the time of this writing, marking the intention of Landis & Gyr to further invest in this technology.

Today, the Landis & Gyr optical card is used in many European countries, including Belgium, the United Kingdom, Austria, Netherlands, Switzerland, Portugal, and Ireland. The United Kingdom has 40,000 pay phones installed. Many other countries in Africa, Asia, and Oceania, including Malaysia, Thailand, and Taiwan operate the optical card system of Landis & Gyr. The optical card has the advantage that no environmental influences—such as electrical fields, electric discharges, or strong magnetic fields—can affect the original optical information or the functionality of the optical code. The security offered to both issuers and users is maximized. No frauds have appeared since its worldwide introduction.

9.3 OPTICALLY VARIABLE GRAPHICS TECHNOLOGY AND VISUAL PERCEPTION

9.3.1 Types of Optically Variable Graphics Elements

OVG elements are produced in many types and for different applications. They are available with full-surface metallization, full-surface transparent dielectric coating, and combinations of both. Depending on whether they are in final form, with or without encapsulation or lamination on a document, the foil system is a hot stamping foil, lamination-heat resistant foil in hot-adhesive, cold-adhesive label version, or a customized version. Together with the great variety of designs and contours this OVG technology offers an extensive diversity of security sol...

In such applications as driver's licenses and police ID cards, which often have to be verified under unfavorable lighting conditions, such as partially diffuse lighting on a rainy or foggy day, the kinegram is ideal. This is attributable to the specific kinegram microstructure, which efficiently diffracts light in the direction of the observer (see Sections 9.4.2 and 9.4.3). Under these conditions, holograms need strong and special light sources and still do not attain the OVG performance.

Semitransparent OVG elements are available as see-through devices to cover information like ID photographs as a security protection. Because of their semitransparency, see-through diffractive devices in general reflect considerably less light to the observer than fully metallized diffractive devices. However, the exceptional diffraction efficiency inherent in kinegram microstructures adequately compensates for this drawback (Section 9.4.1).

Banknote applications are in a category by themselves in matters of requirements and performance. They are at the other opposite extreme from credit card applications, which offer ideal substrate conditions.

9.3.2 Visual Perception Targets for Security Features

The main function of any visual security feature is to provide document protection against counterfeit, imitation, forgery, and fraudulent manipulation. The general public must easily perceive the presence of the feature in any situation. This means that the feature image stimuli must reach the retina. Together with stimuli generated by other image elements, they form the visual information of the document that must be optimally brought into consciousness. The often formulated wish to integrate the feature discreetly within the document leads inevitably to more stimuli processing in the brain than if the feature were allowed to be of striking appearance. These stimuli can receive higher perception priorities than the more discreet but nevertheless very important stimuli. The resulting possible concentration of the authentication on only one security feature could adversely affect authentication. It is a matter of the document security feature portfolio and the importance that the maker and issuer attribute to each of these features that aid in their selection. Discreteness is certainly at variance with effortless and easy perception of a security feature. In the search for relevant psychophysical aspects of visual perception, we will concentrate on the perception of flat objects that are images. In addition, we will focus on OVD-related aspects.

The visual field produced by a graphical image is differentiated into visual figure and background, each having its distinct visual form [14]. Lines can be considered as figures on the ground or they can be seen as edges of areas having surfacelike properties. Studies of perception show that areas produce much shorter neurophysiological signals than narrow and sharp lines. Since the duration of the neurophysiological signals is a measure of how well optical signals are memorized, lines will attract much more attention and imprint the mind much better than surfaces [15,16]. Hence ...

- Crisp sharp lines in a graphic image efficiently help memorization.

Another very important property of human perception is the sensory response to light bursts. Isolated, singular light bursts (stimuli of very short duration) deliver longer impulse activity to the brain than steady or continuously varying light intensities. As a consequence, the sensation of brightness and of visibility is enhanced by short stimuli [18]. This leads to a conclusion for the image variability:

- Best memorization of the variability of an image is achieved when sudden and brisk changes of intensities occur during the image change.

For purposes of memorization, it is advisable to create images of which some elements show an apparent movement (kinematic effect). Such a movement is built up of a sequence of separate phases, much like in animation, as illustrated in Figures 9.1 and 9.2.

In realizing the apparent movement, the designer must consider the fact that the individual phases of the movement are much better perceived if they are composed of lines that produce one intensity flash per phase. In other words, static images as well as continuously varying movements in an image are disadvantageous to perception and memorization. Furthermore, the frequency of those flashes is of importance. As an example, the rotation of the OVD with normal (convenient) angular velocity should produce 8–10 flashes per second. A slowly flickering light may appear brighter than a steady light of the same intensity (Brücke-Bartley or Bartley Effect [17]).

- Designs are made advantageously by integrating picture sequences that produce intermittent flashes of 8–10 Herz when the OVD is normally rotated.

Optimum perception of security features demands application of the above rules to a design. A thorough analysis of perception would certainly result in better understanding of how the design must guide the layman to look for the essential image properties. By applying these rules to the OVG design, optimum visual guidance is aimed at.

9.3.3 Design Concepts and Targets

Ideally, an OVD technique must be able to integrate all possible artwork. The optically variable picture or effect must have certain general properties, which are indispensable:

- Easy to see under virtually any type of lighting conditions.
- Easily and instantly recognizable by the general public.
- Easy to memorize.
- Each effect to be described in few words. Mass media should be able to

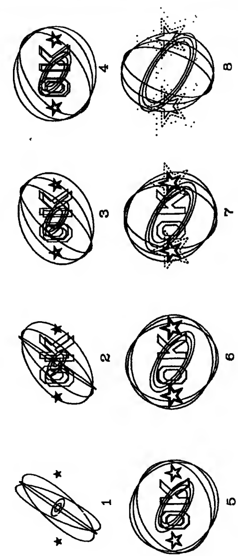

Figure 9.1 The OK Kinegram. This example shows eight selected phases of a series of animated kinematic movements produced by tilting the kinegram.

In the search for a technique able to yield a best possible approach to the rules given in Section 9.3.2, the most difficult problem was to create fine lines with the properties cited. The OVG technique goes beyond the above requirements and ensures that perception rules are implemented. The technique allows for:

- Commensurable variable effects: when tilted, different variable patterns show changing shapes related to each other by a common measure. For instance, in Figure 9.1 a star explodes while the "OK" logo contracts.
- Clear and identifiable movements.
- Quantitative description of the variable effects. Associative and self-referencing elements aiding memorization. When tilted, different figures change (for example, in size) in relation to each other. For instance, in Figure 9.1, once a star has fully collapsed, the "OK" logo appears, fully exploded, the logo vanishes.

The basic idea of the OVG technique is to follow a graphic's artist work. When the artist is drawing lines or filling out areas, the pencil moves across the paper. The OVG technique can best be described to nonexperts by having them imagine that the tip of the pencil is a very sophisticated point that marks the substrate with lines and dots consisting of diffraction patterns. Depending how the pencil is held, the diffraction parameters' spatial frequency and azimuth change. Under the microscope, line cross-over areas are clearly visible (Figure 9.2). This is a significant property of OVG design, which is computer controlled and does not make use of the three-dimensional

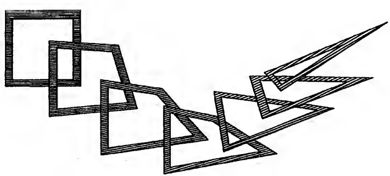

Figure 9.2 Schematic illustration of cross-over areas in a kinegram structure. Various phases are shown of an animated movement along a curved line of an object that changes from a square into an oblong triangle. In this example, the azimuth and pitch of the microstructure increase per phase. Note that the pitch is not to scale but generally varies between 0.7

images of objects or sets of two-dimensional masks that regular holographic techniques apply.

By the virtue of these microstructures and the designed variable effect, the OVG diffracts incident light into prescribed directions. The result is a variable image when the OVG is rotated. The kinematic effects implemented today are: translation, rotation, centrifugal or centripetal radial movement, expansion, contraction, and staggering towards background or foreground. The kinegram (from the Greek word κινειν meaning to move) derives its name from these conspicuous, well-defined movements of graphical elements. The graphics contain lines of any curvature, guilloche patterns, and so on, and are characterized by sharp, crisp, and high precision lines; high contrast; high resolution; measurable and unique movements; and optical effects that are easy to describe. Background patterns of diverse effects add to the gamut of possibilities. Other members of the OVG technology show exclusive flipping characteristics, distinctive synthetic shadow structures, or dynamic gloss effects, depending on whether a representation of a nonexisting object has been chosen by the client. The dynamic effects thus obtained are of infinite variety and accommodate any graphist's desires. Furthermore, Mandelbrot fractals are an OVG design variant, while background areas or lines can be filled with or infrastructured by alphanumeric microwriting.

9.4 ELEMENTS OF OPTICALLY VARIABLE GRAPHICS PHYSICS

9.4.1 The Light Diffraction Aspect

OVG technology is an application of the physical phenomenon of light diffraction (Chapter 3, Section 3.3.3), in particular, from reflective phase gratings. Generally, this subject is treated as a so-called *direct problem*. First, an optical configuration of light sources and diffractive structures is defined; subsequently, the resultant propagation of radiation towards the observer is calculated. Conversely, OVG technology makes use of the inverse procedure by solving *inverse problems*, which involve the definition of a desired visual effect and the subsequent calculation of a combination of light sources and diffractive scatterers, which produce this required effect by steering diffracted light beams in the required directions [10,11]. Thus, it is possible to compose a kinegram image consisting of multiple juxtaposed gratings that direct tens to hundreds of diffraction orders equally divided over its complete hemisphere. As a result, the observer of a kinegram will see iridescent diffractive effects virtually independent of the angle of illumination and observation [13]. In contrast, holograms diffract very few orders into the observers' space and do not show iridescent effects under many lighting and observation conditions. What is seen when looking at a kinegram is light scattered from its surface through light diffraction by the various reflection phase gratings. The

show no iridescence. For a fixed set of lighting and observation angles, particular areas will diffract more light towards the eye than others. If these angles are varied, the perceived light intensities will vary. Because the eye concentrates on high-intensity areas, the effect is the perception of moving elements (Section 9.3.3).

It must be emphasized that, from a standpoint of visual inspection, this is the power of the kinegram: it displays well-defined kinematic effects, independent of lighting and observation conditions, that may be easily memorized. Conversely, holograms rely on their attractive but hard to define three-dimensional characteristics for visual inspection and on their obvious but poorly defined display of variable colors, which depend to a great extent on conditions of lighting and illumination.

9.4.2 The Diffraction Structure Aspect

When the results of the inverse calculation (Section 9.4.1) are available, the problem rests in making the required three-dimensional profile microstructures. The parameters calculated are spatial frequency, azimuth, and section profile of the microstructure [19]. Today, many technologies are used with varying success. The most successful method is the traditional optical exposure of photoresist with regular grating structures, resulting in a sinusoidal section profile of the grating. More sophisticated methods must be used if more than the regular sinusoidal section profile microstructures are demanded. To this end, many possible techniques are available, from chemical differential etching to ion beam etching procedures and from traditional electron beam lithography to very sophisticated electron-beam modulation techniques. We have to make sure that all processes involved in the OVG technology are irreplaceable by other, cheaper alternatives, resulting in indistinguishable products. Any attempt to shortcut processes should inevitably be clearly recognizable as an illicit replication. It must be emphasized here that nonsinusoidal gratings can, on principle, not be copied by optical holographic replication means, as discussed in Chapter 8, Section 8.3.4. The larger part of the counterfeits falls in this category.

The reader will certainly understand that we do not disclose our methods to produce the structures used in the OVG technique. The computer-aided large-scale diffraction grating synthesizer we have developed makes use of a bank of microstructures whose diffraction properties have been calculated. Depending on which visual effect is to be created in the OVG image, selection is made of the diffraction properties needed. The OVG technology makes use of the possibility to modulate diffraction intensities or steer light beams in the desired directions depending on the effect targeted.

From the standpoint of durability, it is of paramount importance that functional diffraction properties are integrated in an OVG image, particularly if the substrate is going to suffer crumpling or folding. A wrinkled surface shows statistical angular fluctuations and thus the angles of lighting and observation to the normal on the surface fluctuate arbitrarily. As a result, the diffracted colors vary over the surface in an undefined way and thus cannot contribute to reliable visual inspection. The designed kinematic effects of a kinegram, however, are controlled by the rotation of its surface and are highly independent of conditions of lighting and observation. Moreover, by rendering the distribution of diffraction properties of the grating composition redundancy, the effect of crumpling is further reduced and therefore does not have a severe influence on the projected kinematic effects.

Durability requirements are at variance with security considerations, which imperatively demand an irreversible destruction of the feature if it is manipulated for fraudulent purposes. A fine balance had to be found in the choice of the materials entering the OVG production process. It is known that banknote durability requirements are among the most difficult conditions to fulfill, especially in the context of film devices to be affixed on the paper. For all other document protection functions, the banknote has been said to be a pièce de résistance application. The durability tests performed at Landis & Gyr have been documented [5]. Today, the results of the resistance of the kinegram on Austrian and Finnish banknotes in circulation show that the kinegram performs to the expectations. It is common practice among banknote issuers to withdraw used notes from circulation and replace them with new ones. The permissible degree of wear is different from issuer to issuer. We do not know of any case where the kinegram has been the reason to withdraw a normally used note from circulation. The crumple resistance of the kinegram has been shown to be excellent on Finnish as well as on Austrian banknotes. The abuse tests, laundering, crumpling, soiling, abrasion, and chemical resistance, are classical for banknote applications. We have added the tests of carbonizing and aging. In any other application, the testing procedure is finalized with the client. The specification list of the materials used to produce OVG elements carries the name of the specification, the test procedures, and the instruments to be used, and the values and the tolerances required.

9.4.3 The Difference between Holograms and Optically Variable Graphics

Holography is suffering today from having delivered all it was capable of for security and product identification. Holographers are faced with the problem of having to quit very soon the hologram stand-alone security device market. There are pertinent reasons for this situation. We have always maintained that the holographic technology's inherent low security reserve and its poor technical upgradability potential is clearly insufficient for security applications. Mass media have wrongly talked about high tech in the context of holography. It has taken just a few years to prove our projection. Today credit card issuers are facing the first mass counterfeits. The relatively simple holographic technology has permitted a widespread use of the technique

and has enabled counterfeiters to practice the technique with success. More so, holographers have themselves precipitated this development by publishing ways and means to counterfeit holograms [12] and by a worldwide selling of the holographic embossing technology.[1] By doing so, they have provided an early disqualification of holographic stand-alone security devices. (Editor's comment: For an alternative view on advanced holographic security features, see Chapter 8, Section 8.3).

With the exception of computer-generated holograms, holograms are optical records of a three-dimensional physical object or model. The recording and reconstruction procedures of the rainbow-type hologram, visible in white light are well known (Chapter 3, Section 3.4.2) and a mathematical treatment can be found in many textbooks. Compared with the OVG technology, there are striking differences [6,7]:

- Holography is a technique whereby diffusely scattered light waves of a physical model are recorded on light-sensitive materials. The reconstructed model diffusely scatters light in all directions. As a consequence, any point of a hologram diffuses incident light into a wide range of angles. This results in a loss of useful light intensity (Figure 9.3), giving rainbow holograms their slightly milky look. Furthermore, it must be observed that security holograms are generally multicolor holograms (Chapter 3, Section 3.4.2); the superposition of multiple holographic images reduces their diffraction efficiency.

  OVG technology depends neither on light recording techniques nor on the superposition of multiple images. The OVG image is computer generated, does not need a physical model, and therefore does not suffer light losses by diffuse scatter. All of the juxtaposed OVG elements very efficiently diffract light in the direction of the observer's eye (Figure 9.3). OVG elements look crisp, brilliant, and sharp.
- The holographic recording and reconstruction methodology allows only a limited number of diffraction orders to be projected in the observer's space. As a consequence, the holographic reconstruction is only available for adequate inspection and authentication under well-defined angles of lighting and observation.

  OVG design allows the efficient projection of many diffraction orders into the main part of the observer's space. Therefore, the kinegram image can be inspected and authenticated under almost any angle of lighting and observation (Section 9.4.1).
- Hologram images suffer severe degradation of their reconstruction when they are crumpled because the irregular surface causes the diffracted colors to vary arbitrarily (Section 9.4.2). This lack of well-defined color rendition is inherent to crumpled holograms and is insuperable. Additionally, the above-mentioned light loss due to diffuse scatter and image superposition tends to reduce the diffraction efficiency of a worn hologram to inadequate levels in a relatively early stage.

  OVG elements are designed to withstand considerable crumpling because their projected kinematic effects are highly independent of surface irregularities (Section 9.4.2). Furthermore, the perceptibility of the diffracted effects is preserved for a relatively prolonged period of use and wear, thanks to the optimum diffraction efficiency of juxtaposed kinegram gratings.
- Holograms are not capable of displaying the optical effects that satisfy the perception rules Section 9.3.2 discusses—in particular, the intermittent flashing frequency of separate image elements.

  Conversely, OVG elements are designed to display all optical effects that comply with the relevant psychophysical perception rules.
- Holographic recordings merely consist of the more or less sinusoidal phase gratings characteristic of optically recorded gratings (Section 9.4.2). The diffraction properties of optical holograms are limited to the performance of these structures and can be copied by various holographic techniques (Chapter 8, Section 8.3).

  OVG technology makes use of all types of nonholographic gratings, provided they can be physically originated. The microstructures required for particular optical effects are derived by inverse calculation (Section 9.4.1). Such structures cannot be copied by optical techniques.

[1] See for instance, the advertisements of Global Images Inc. in *Holographics International*, Spring Issue, No. 3, 1988.

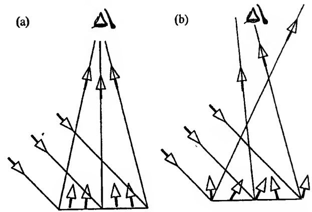

Figure 9.3 Schematic illustration of (a) *inverse scatter* of OVG elements and (b) diffuse scatter of a holographic image.

9.5 MACHINE READABILITY OF OPTICALLY VARIABLE GRAPHICS SECURITY DEVICES

For institutions that run communication networks that use optical security documents, machine readability of the security document is only one piece of the system. From the very beginning of planning such a system, a clear concept of needed data, data flow, and data treatment must be established. Additionally, the specifications of where, to what extent, and how the data must be protected must be established. In most cases, the required system performance specifications take into account secured or nonsecured data, terminal type, host used, communication requirements, and other hardware and software to be used. This section restricts the discussion of machine readability to reading of optical information available from a document. It does not treat the further processing of signals or data within a system, although this is of paramount importance.

Machine readability of optical information concerns two basic types, secured and nonsecured optical information. Table 9.1 lists the type of optical information available in principle from a machine-readable document for three sample cases.

The machine readability of secured optical information covers the overt and the covert type, whereas both types are subdivided into noncoded and coded information. A complex situation arises if mixes (superpositions, juxtapositions, or both) of above information types are used. The word *coded* can but does not necessarily involve cryptographic secrecy or ciphering. It can also mean a form of information accessible to machine reading. The reading of secured optical information can serve the purpose of authenticating genuine optical properties of the OVG element, the gathering of data

Table 9.1
Parameters of Machine Readability (Three Document Types)

Parameters	*Case 1*	*Case 2*	*Case 3*
Overt	No	Yes	Yes
Covert	Yes	No	No
Congruent and identical with visible OVG signals	No	No	No
Juxtaposed and mixed across entirely of OVG	Yes	Yes	No
Juxtaposed to, but outside OVG picture	No	No	Yes
Superposed across entirety of OVG	No	No	No
Coded	No	Yes	Yes
Noncoded	Yes	No	No
Cryptographic	No	No	No
Noncryptographic	Yes	Yes	Yes

enabling the identification of the element in connection to its substrate, or the simple reading of unalterable data.

OVG elements containing overt, noncoded optical information (as available from printed intelligible information, such as pictures, images, text, and so on) can be machine authenticated. However, if complete congruence is to be realized between human-perceived and machine-tested authenticity, the task is extremely difficult, time-consuming, and costly. It relies on standard pattern recognition techniques adapted to OVG patterns and supplemented by genuinity tests. Even for high security applications this is not asked, since a complete one-by-one, signal-to-signal congruence between human-perceived and machine-read signals does not significantly contribute to higher security/cost ratios. For extreme security applications in which cost is a less determining factor, this congruence is a must. In the case of OVG elements as the kinegram, we have not developed the case of complete congruence because it does not correspond to profitable needs in today's market.

Case 1

The first solution offered in Table 9.1 consists of intermixing the OVG image with statistically dispersed incremental elements—tiny diffractive elements that contain the minimum number of necessary grooves (approximately 10–15), which are readily accessible to machine sensing but do not disturb the overall picture. Thus it is ensured that any fraudulent attack on the OVG itself recognized by the observer would inevitably lead to a net change in machine-readable characteristics and, in consequence, to document rejection. The efficiency of the method relies on the resolution of the scanner and the surface scanned. Although disputable in matters of semantics, we classify this method as being of the covert, noncoded, noncryptographic type rather than the overt. Case 1 entirely addresses the automatic checking of the authenticity of the OVG on its genuineness. It is, of course, realized that strictly speaking, the OVG's perceptual impression on the eye is not really checked by the machine. The probability that a fraudulent attack on the OVG is detected by the machine is nevertheless extremely high and certainly higher than the probability of visually detecting it.

Case 2

In the case of reading overt, coded optical information (as realized with visible bar-codes), the pure OVG part is naturally overt but the coded optical information can be added to the OVG by mixing incremental coded information into the picture. The result is an OVG covered by a visible machine-readable bar code across the full picture. In this case, complete one-to-one congruence of the visible OVG signals and the machine (bar code) signals cannot be achieved. The result is, nevertheless, a highly

of the OVG inevitably harms the machine signals. This type of machine-readable OVG has been realized in a feasibility study for banknote applications in which banknotes must be read in high-speed authentication machines at speeds of up to 60 notes per second.

Case 3

Where it is possible, useful, and acceptable, one would wish for the purpose of simplicity to dissociate the machine-read surfaces from those carrying the OVG information. This can usually be best realized by juxtaposing or adding to the picture machine-readable information arranged in a track for this purpose. This track can be placed along the frame of the OVG and outside of it. It is visible but coded, either with or without cryptographic ciphering, depending on the application. A Landis & Gyr technique that is similar, although more sophisticated and of covert type, has been in use worldwide for many years for prepaid telephone cards.

REFERENCES

[1] Landis & Gyr Review 1 (1980).

[2] Prange, O., "KINEGRAMS wage war on forgeries," *Network*, No. 6, 1991, edited by Frontpage, Zurich, Switzerland.

[3] Moser, J.-F., "KINEGRAM® Technology," *COMECON Conference on Issuing of Banknotes*, Budapest, Hungary, May 21–26, 1990.

[4] Moser, J.-F., "The Learning Curve in KINEGRAM® Production," *Banknote Printers Conference*, Zurich, Switzerland, May 21–24, 1989.

[5] Moser, J.-F., "The KINEGRAM®, a New High Security Optically Variable Device," *Optical Security Systems International Symposium and Product Presentation for Optical Information Storage and Display*, Zurich, Switzerland, October 14–16, 1987.

[6] Antes, G. P., "Holograms and Kinegrams as Visual and Machine-Readable Security Features on Securities and Plastic Cards," *Proceedings of the International Symposium on the Stability and Conservation of the Photographic Images, Chemical, Electronic and Mechanical*, Bangkok, Thailand, November 3–5, 1986, ed. by The Society of Photographic Scientists and Engineers, 7003 Kilworth Lane, Springfield, Virginia 22151, U.S.A., pp 24–33.

[7] Antes, G. P., "Holograms and General Light Diffracting Devices, State of the Art, Applications, Trends, and Limitations," *Proceedings of the International Symposiumon the Stability and Conservation of the Photographic Images, Chemical, Electronic and Mechanical*, Bangkok, Thailand, November 3–5, 1986, ed. by The Society of Photographic Scientists and Engineers, 7003 Kilworth Lane, Springfield, Virginia 22151, U.S.A., pp 85–94.

[8] Moser, J.-F., "Developments in Laser Techniques," *International Masters Printers Associa-*

[9] Moser, J.-F., "Technical Highlights of the New Security Features," *Proceedings of the One-Day Symposium on New Security Features for Banknotes and Security Papers*, Palace Hotel, Lucerne, Switzerland, 29th October 1981.

[10] Baltes, H. P., (ed.), "*Inverse Scattering Problems*," Berlin, Heidelberg, New York: Springer-Verlag, 1980.

[11] Baltes H. P., (ed.), "*Inverse Source Problems*," Berlin, Heidelberg, New York: Springer-Verlag, 1978.

[12] McGrew, S. P., "Hologram Counterfeiting, Problems and Solutions," *SPIE Vol. 1210 Optical Security and Anticounterfeiting Systems*, 15–16 January 1990, Los Angeles, California, pp. 66–76.

[13] Antes, G., "Dokument mit einem beugungsoptischen Sicherheitselement," Landis & Gyr Zug AG, Zug, Switzerland, *patent number EP 0 105 099*, April 4, 1984.

[14] White, D. A., Ward, J. P., Bartley, S. H., "Visual Form: A Reassessment of the Vocabulary in Scientific Psychology," *Psychological Record*, Vol. 38, 1988, pp. 67–76.

[15] Bartley, S. H., "Some Relations between Optometry and Psychology," *American Journal of Optometry & Archives of American Academy of Optometry*, Vol. 50, 1973, pp. 521–532.

[16] Bartley, S. H., "Some Sensory End Results and the Activity of the Optic Pathway," *American Journal of Optometry & Archives of American Academy of Optometry*, Vol. 41, 1964, pp. 362–370.

[17] Bartley, S. H., "Subjective Brightness in Relation to Flash Rate and the Light-Dark Ratio," *J. Exp. Psychol.*, Vol. 23, 1938, pp. 313–319.

[18] Trauzettel-Klosinski, S., and Aulhorn, E., "Measurement of Brightness Sensation Caused by Flickering Light," *Clin. Vision Sci.*, Vol. 2, 1987, pp. 63–82.

[19] Antes, G. P., "Beugungsoptische Mikrostrukturen als Informations und Echtheitselemente bei Wertpapieren, Geldersatzsystemen und anderen Anwendungen, *Kolloquium für Photographie und Bildwissenschaft, Eigenössische Technische Hochschule*, Zürich, Institut für Kommunikationstechnik, July 16, 1987.

Chapter 11

Iridescent Optically Variable Devices: A Survey

R. L. van Renesse

11.1 INTRODUCTION

Optically variable devices (OVDs): without exception the chapters in this book either refer to them or treat them extensively. OVDs have become a much debated cornerstone of optical document security. Generally, the concept is confined to devices exhibiting iridescence, discussed in Chapter 3, Section 3.3. The concept, however, has also given rise to Chapter 15, which discusses noniridescent OVDs in an effort to counterbalance the disproportionate amount of attention currently drawn to iridescent effects in the context of document security. This current attention is also reflected in the entire book; several chapters are devoted to this current matter. As a balance, other chapters extensively treat paper security, security printing techniques, and noniridescent security overlays.

Diffractive structures can be divided into first-order devices (such as holograms) and zero-order devices. Interference structures, in their turn, can be divided into single layers (pearl luster pigments) and multilayers (Bragg structures, thin film stacks).

The iridescent effects of diffraction and interference present a charming play of varying colors with angle of observation, which the layperson generally considers to constitute the whole security effect: easy first-line control and color copy protection. Any iridescent device will do that job. But there is rather more to it. The reader of this book will find that, almost invariably, the producers of one device tend to maintain that their device is superior to any other existing device and produce more or less convincing evidence of it. This can cause the reader some bewilderment. It is the purpose of this chapter to discuss and compare the main pros and cons of these various iridescent devices.

11.2 HOLOGRAMS

In Chapter 3, Section 3.4.2 the principle of holography is briefly explored. The iridescent color shift and three-dimensionality of holograms have not only been considered a visual fascination but also a security aspect because of their conspicuousness. But it is also true that such elements can divert the attention of the examiner from other vital security features. The diverting effect of iridescence, of course, holds for all types of iridescent security features. Sometimes the luminous dominance of the OVD has even been deliberately decreased to better assimilate the OVD with the document's overall design.

11.2.1 Volume-Reflection Hologram Overlays

Volume-reflection overlays are multilayer structures of the Bragg type and have been proposed for security purposes by Ilford [1] under the trade name *Flashprint*. These overlays are highly transparent but under a specific angle of illumination and observation a very bright reflective gold-to-green image is displayed that is up to eight times brighter than white. The brightness of its display allows it to be placed over white paper without the whiteness of the paper pushing away the iridescent effect. This latter effect appears with pearlescent and liquid crystal overlays and some all-dielectric thin film devices that therefore demand a black or rather dark background. This brightness, however, is obtained at the expense of Flashprint's viewable angle, which is extremely small. This can be considered a serious drawback of an OVD, which should display its characteristic iridescence under a large range of lighting and viewing conditions. Various solutions developed to realize the required large angular visibility of iridescent effects are discussed here.

When viewed under uncontrolled lighting conditions, Bragg structures exhibit a more predictable color than diffraction gratings. It is indeed the unpredictability of the color display under arbitrary lighting that is sometimes considered a disadvantage of embossed gratings and that various authors propose different solutions for. Even under highly diffuse illumination, where first-order diffractive devices completely fail, Flashprint appears to display a rather bright Bragg reflection with a well-defined saturated color.

The volume-reflection recording setup generally provides an angular offset between specular reflection by the substrate and diffuse object reflection. As a result, the multilayers do not quite line up parallel with the substrate, so that on reconstruction the reflected interference colors are not disturbed by the specular reflection of the substrate.

Making reflection holograms demands professional skill, but it can be done in a relatively simple "homemade" holographic set-up. The reproduction risk of volume

holograms, therefore, is not at all imaginary. A major drawback, however, of volume-reflection holograms is that their mass fabrication is still unduly expensive. Ilford, therefore, never made a market for Flashprint and the practical application of volume-reflection overlays to document security has generally remained insignificant.

11.2.2 Embossed Rainbow Holograms

Embossed rainbow holograms can be mass produced at very low cost and were the first iridescent OVDs applied for security documents (Chapter 8, Section 8.1). The complete process, including shim fabrication and embossing [2], demands more than a homemade setup. It has been argued that the holographic embossing technology has been sold out by the holographers themselves (Chapter 8, Section 8.3.1 and Chapter 9, Section 9.4.3) and requires advanced procedures to provide protection against illicit reproduction. Chapter 8 and [3] discuss these advanced holographic techniques.

Apart from iridescence, a major security item of holograms is considered their 3-D image content, in particular 3-D human portraits (Chapter 8, Sections 8.3.1 and 8.3.2). Their scrutiny demands the complex process of visual image recognition. It has been argued by various authors that the human face serves some security value, in particular when it concerns well-known persons. Humans beings are imputed to have a particular ability to recognize human faces; a specific location in our brains appears to be devoted to this task of visual perception and therefore small deviations of the original are easily observed. Conversely, it is argued in Chapter 7, Sections 7.2 and 7.5, that the visual system compensates for such deviations and that even severe anomalies may remain unobserved. Actually, even grossly distorted portraits are recognized without effort, the distortions frequently remaining subconscious. This may cast some doubt on the practical value of this complex recognition task for first-line security. In fact, this whole theory appears to be nothing but a myth that has been traditionally entertained in security circles without any substantiation whatsoever. Furthermore, practice teaches that people hardly ever scrutinize complex details, whether three-dimensional or two-dimensional—if they know at all what details to look for!

Characteristic of rainbow holograms is that they project a slit-shaped first-order beam into the observer's space. This renders this type of hologram a rather limited angle of observation. Most security embossings, however, have been made with multiple reference beams and project at least three first-order slits under different angles. In white lighting these slits smear into spectra that overlap to cover a considerable angular space.

Multiple holographic exposures, however, suffer decreased diffraction efficiency, because the exposures spatially overlap and the corresponding image elements thus have to share the amount of incoming light. To avoid this deficiency, multiple

holographic exposures are frequently given via variously shaped physical masks; this is a cumbersome procedure that limits the freedom of design and is attended with obvious adjustment difficulties.

In contrast, the juxtaposed diffractive grating elements of, for example, pixelgrams and kinegrams each optimally diffract the incoming light to create optically independent image elements. Additionally, due to the diffuse nature of the holographed models, the brightness of rainbow holograms can be substantially lower than that of specific grating-type securities like kinegrams and pixelgrams. Although under normal lighting conditions holograms display sufficiently bright images, this hampers their inspection under low-level lighting conditions (for example, evening public transport, bars). Additionally, the unsharpness of 3-D images when illuminated with extended light sources (for example, fluorescent tubes, overcast sky) has been put forward as a drawback of holograms. In the case of fluorescent tubes, this drawback is negligible, but an overcast sky completely spoils the 3-D holographic effect as well as the variable color display.

Other disadvantages of rainbow holograms that have been put forward are the sensitivity of their iridescent display to the angle of lighting and observation and their hard to define color display under complex lighting conditions. Their angular sensitivity results in considerable *color mottle* and even in local *switching off* of the reconstruction, which renders hardly recognizable images due to the small and random variations in surface angle caused by crumpling. The cause of this critical performance is the small angular extension of the slit that is reconstructed in the observer's space. Local angular surface deviations due to crumpling deflect the slit partly or wholly out of the observer's view. Of course, this drawback only pertains to applications on paper substrates and is not relevant to stiff documents like plastic cards. The advocates of special security gratings like pixelgrams and kinegrams claim solutions for this sensitivity to crumpling that depend on the distribution of multiple gratings with varying grating period and azimuth over the feature's surface so that the observed phenomena become highly independent of the color displayed. And indeed the only diffractive securities found on banknotes nowadays are multiple gratings like the kinegram (Austrian 5000 Schilling, Finnish 500 and 1000 Mark) and the prototype pixelgram (Australian $10, Singapore $50 plastic notes), while otherwise various types of holograms are only found on plastic cards.

The ordinary rainbow hologram shows iridescent effects in the sense that, on tilting it, the spectral colors are displayed in order. This may seem a good and simple description, but this order is generally unknown by laypersons. Additionally, this becomes complicated in the case of multiple-slit security holograms and even more if the lighting consists of multiple sources, extended sources, or both. The rainbow color display is not simply definable but with the vague observation that it is optically variable. A simple and adequate description of the 3-D image content can also bear difficulties. It may be simple to say that the image contains a dove (VISA) or a portrait

seems simple and an embossed hologram of it would do the job to the satisfaction of the criminal. The reproduction of a portrait of a celebrity might seem more difficult because the counterfeiter would have to get hold of the celebrity in person to fabricate the desired reproduction. But is this person on the Eurocheque really Beethoven or just a model? And cannot all celebrities be modeled? It can be doubted if anyone would get suspicious.

In contrast, an adequate first-line security would require a simple and unambiguous description. Kinegrams and pixelgrams are claimed to meet this requirement by reverting to alternative effects (kinematic effects and positive-negative swap) and abandoning optically variable colors as well as three-dimensionality as specific security items.

Finally the aspect of machine inspection has to be regarded. It is of course possible to detect the various diffraction orders of a rainbow hologram by dedicated optical equipment as an indication of its presence. But the presence of diffraction orders in a specific angular space is not very discriminative and this condition could be satisfied by diffractive structures that do not even show the faintest visual resemblance with the genuine feature. A more rigorous approach might be the image-wise sampling of the 3-D hologram reconstruction and applying image recognition techniques. This approach, however, is very complex, expensive, and slow and it is not fit for fast machine inspection (for example, in the order of 40 or more documents per second). If machine inspection of holographic features is demanded, the feature can be provided with additional 2-D grating structures (either overt or covert), but of course this excludes inspection of the complex holographic image itself.

Assessment of the security benefits of holograms must take into account that Gabor did not invent the hologram in 1947 for the purpose of security. It was not even invented for its remarkable 3-D characteristics, although these made it famous. Its possible application to security was realized only in 1979 (Chapter 8, Section 8.1), long after its invention and even long after the invention of the laser in 1960. In the meantime, additional security has been added to the embossed hologram, which has turned it into a useful optical security device.

11.3 MULTIPLE GRATINGS

Chip technology spin-offs, such as electron beam lithography, vacuum deposition, and ion beam etching, allow the sculpture of matter with nanometer precision. Matter has become a virtually unlimited recording medium that is only beginning to reveal its seemingly magic potential. As a result, diffractive elements can be "carved" into matter, consisting of a multiplicity of gratings, juxtaposed with extreme precision. Period, azimuth, and profile of groove patterns can be shaped at will so that unexpected and highly uncommon optical effects result that are extremely difficult to counterfeit,

techniques. Additionally, computer graphics aid design of sophisticated pictorial effects based on these novel optical phenomena.

Although simple multiple gratings can be created by multiple exposures of optical light beams, the more advanced types are not. Multiple gratings either consist of:

- An assembly of variously shaped diffractive picture elements, such as alphanumerics, logos, microprint, and guilloches, (kinegrams, zero-order structures), each with a specific period and azimuth of the grating lines it contains;
- An assembly of equally shaped pixels in a regular matrix, each with a varying grating period and azimuth (pixelgrams).

The manufacturing technique allows a virtually theoretical diffraction efficiency, which may therefore be considerably higher than that of holograms. This should not only be an advantage under dim lighting but also in case of semitransparent overlays, which, to expose the printed information, have a substantially lower reflection than fully aluminized opaque devices. An exception is the zero-order device, which reflection does not depend on metallic coatings (Section 11.3.4). It must be noted, however, that diffraction efficiency of these thin structures depends also on the smoothness of their substrate, which can vary from a smooth pvc card to a rough paper. In particular, the random microstructure of paper fibers tends to have a detrimental effect on the perceived brightness of diffractive structures. Comparisons of performance therefore can be made only under comparable conditions.

11.3.1 Kinegrams

Shortly after Colgate's revelation in 1979 (Chapter 8, Section 8.1.1), Gregor Antes of Landis & Gyr [4] realized that holograms do not fulfill all requirements that security devices should meet, in particular, independence of lighting and resistance against the optical effects of wrinkling. To this purpose, Landis & Gyr developed the kinegram, which, contrary to the hologram, is exclusively designed for top security purposes (Chapter 9). The kinegram concept intentionally abandons three-dimensionality as well as optically variable color display, considering them inadequate as security ingredients. Kinegrams do not become unsharplike holograms in case of illumination with extended light sources. They do display iridescent colors, but these are not considered essential security items. Because of the absence of 3-D, holographers tend to consider kinegrams (as well as pixelgrams) as flat art, standing at the lowest level of optical security along with ordinary 2-D holograms. This will be shown to be a misconception.

Instead, kinegram security is based on a variety of kinematic effects, like swapping, rotating, moving, exploding, and imploding graphical image elements. Such kinematic effects can be simply and unambiguously described. Microscopic

specific kinematic effect consists of a grating with a specific period and azimuth. It can thus be seen in only one condition of observation. The next phase of the kinematic animation is displayed by a nearby diffractive element with a specific period and azimuth but different from that of the former element. This element comes into view after further rotation of the kinegram. Thus each element in its turn appears and disappears as an animation phase on rotation of the substrate, which renders a kinematic effect (Figure 11.1). The visual perception and recognition aspects involved are treated in Chapter 9.

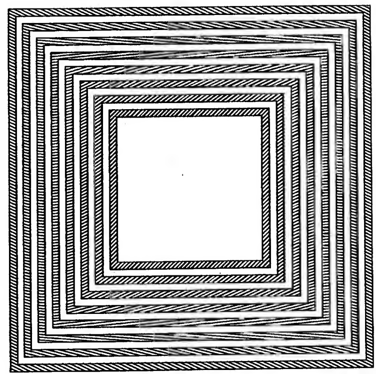

Figure 11.1 Kinematic effect: exploding square. In this schematic illustration, the kinematic image element is a square that consists of eight diffractive subelements. The size of the element is in the order of millimeters. For clarity, only a few grooves are presented; in reality, the image elements contain many thousands of grooves that can only be seen through considerable microscopic enlargement.

In their turn, holographers have endeavored to mimic kinematic effects. Current examples are the Movigram™ and the kinematic effects created by Light Fantastic.[1] The holographic designs appear to be inspired by original kinegram designs and demonstrate the aroused interest in kinematic effects for security purposes. However, holographic kinematic effects are based on multiple exposures of 2-D or 3-D objects, a procedure attended with the noticeable drawbacks described in Section 11.2.2. Kinematic effects can also be created by multiple interferometric exposure of tiny, more or less uniformly shaped grating patches with varying period and azimuth [5]. This procedure does not suffer the disadvantages of holography, but the freedom of design and the variety of possible optical effects are limited as well.

Through careful choice of the distribution of grating period and azimuth over the various diffractive elements, the kinegram can be designed so that diffraction orders cover the main angular space of the observer (Figure 11.2). As a result, diffractive effects are visible largely independent of lighting and observation angles. In this kinegrams succeed better than holograms, even if the latter project multiple slits into the observer's space. The kinegram thus attains considerable independence of lighting conditions. However, under an overcast sky all diffractive orders expand and overlap so that kinematic effects are largely lost. This loss of unambiguous diffractive effects under diffuse illumination is a characteristic of all first-order diffractive devices, whether holograms or multigrating-type structures, although the latter type tends to perform better under diffuse lighting.

The claimed kinegram resistance against the optical effects of wrinkling (Section 11.2.2) is based on the independence of the kinematic effects of angle of lighting and observation. Unfortunately, no comparative investigations have yet been published that support this claim. However, from this description of kinematic image elements (Figure 11.1), it will be clear that crumpling will not easily destroy the visibility of an image element because it embodies a number of subelements with different grating attributes. Thus the image element will be seen under a great variety of angles of illumination and observation. On the other hand, crumpling will obviously tend to distort the kinematic effect. Alternatively, static image elements that do not contribute to kinematic effects, can be composed of tiny diffractive elements that contain the minimum number of necessary grooves (approximately 10–15) to create an adequate diffraction effect. Such *incremental elements* can consist of gratings with statistically varying parameters that cope with the detrimental effect of crumpling.

Holographers report routine optical replication of most rainbow hologram embossings, kinegrams, and pixelgrams, a finding confirmed by the authors' experiments. It must be observed, however, that security kinegrams can be provided with nonsinu-

[1]Movigram™ is a product of Hologram Industries, 42-44 Rue de Trucy, 94120 Fontenay-sous-Bois, France. The address for Light Fantastic is ELEF, PLC Unit 4, Gelders Road, Shepshed, Leicestershire LE12 9NH, United Kingdom.

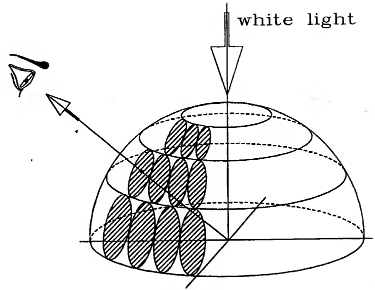

Figure 11.2 Schematic illustration of many diffraction orders equally divided over the complete hemisphere of the observer's space. (After [4].)

soidal grating structures. Such structures (for example, sawtooth-shaped gratings) display diffractive effects that can be neither produced nor copied by purely holographic means (Chapter 9, Section 9.4.2). A brief investigation of any rainbow hologram will reveal that the plus and minus first orders (reconstructions on either side of the zero-order specular reflection) are completely identical. It is well known that sawtooth (*slanted* or *blazed*) gratings [6] diffract most incoming light into only one order. Blazed gratings are manufactured for spectroscopic equipment, but the principle can be applied to security gratings. Such gratings will show distinctive differences between the plus and minus first-order diffraction, easily visible with the naked eye. The effect is uncopyable by holographic replication techniques.

It will be clear that the diffraction structures discussed are well suited for various kinds of machine reading, either of overt or of covert information. Chapter 9, Section 9.5 treats this subject.

Summarizing, kinegrams present sophisticated pictorial designs and constitute highly valuable security devices for first-line as well as machine inspection. Contrary to the conviction of holographers, the opinion exists that kinegram security compares

favorably with that of holograms [7]. Kinegrams are applied worldwide in a variety of security documents.

11.3.2 Pixelgrams

The pixelgram is a development of the Commonwealth Scientific and Industrial Research Organization (CSIRO) in Australia and is described in several patents and papers [8–10]. The prototype of the pixelgram appeared on the Australian ten-dollar commemorative plastic note, issued in 1988. It consists of an embossed multiple-diffraction grating containing a portrait of Captain Cook, whose face is built up of a regular matrix of similar and uniformly shaped diffraction gratings, called pixels, which in the prototype are visible with the naked eye. Like the kinegram, and for the same reasons, the pixelgram design intentionally abandons holographic three-dimensionality (see Appendix A).

Microscopic observation of advanced pixelgrams shows that each pixel (60–125 μm square) is composed of numerous (approximately 30–100) diffraction grooves that continuously vary in period and azimuth. Pixels corresponding to bright areas of the picture contain more strongly curved grooves than dark pixels. It can be appreciated that virtually curvilinear equidistant grooves project diffraction orders with a very limited angular dispersion into the observers space and will therefore remain dark under most lighting and observation conditions. In contrast, pixels with strongly curved grooves of variable period project expanded diffraction orders into the observer's space and will thus be perceived as bright under most circumstances. If, however, the pixelgram is observed under such an angle that the "dark pixels" light up, they will display a much stronger brightness than the "bright pixels," which have their diffracted light smeared over a considerably larger angle in space. Consequently, the appearance of the image will switch from positive to negative. This positive/negative swap is considered a simple first-line security test.

The pixels with strongly curved grooves offer the advantages of a large angular-diffraction effect visibility as well as a decreased susceptibility to crinkling as long as the crinkling angles do not exceed the angle of expansion of the diffracted beam. A schematic illustration of the possible courses of the grooves is given in Figure 11.3. Obviously, the pixelgram and the kinegram offer comparable solutions to the optical effect of crumpling: the composition of image elements of subelements with varying grating parameters.

The human portrait is a principal security feature of the pixelgram because of its conjectured easy recognizability; this time-honored security consideration is frequently applied to banknotes. The grating attributes are chosen to represent the various shades of the original photograph. Apart from the portrait, visual security characteristics of the pixelgram are its optically variable colors and the positive/negative swap.

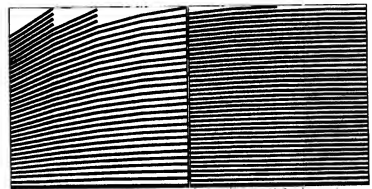

Figure 11.3 Schematic illustration of the course of grooves in two different pixels of the pixelgram. The size of the pixels is near or below the resolution of the naked eye (approximately 0.06–0.125 mm). (a) Strongly curved grooves corresponding with bright pixels. (b) Virtually curvilinear grooves corresponding with dark pixels.

allow a straightforward description. The variable color display, however, cannot be unambiguously defined.

With reference to the Austrian 5000 Schilling kinegram, the pixelgram is claimed to be superior over the kinegram, which "only produces schematic types of images" [9]. Evaluation of this assertion must take into account the doubt that can be cast on the security value of human portraits (Section 11.2.2). Furthermore, the kinegram design concept is based on disparate considerations of visual perception and aims at kinematic effects of sharply outlined line elements, which would offer better memorization than static images consisting of extended image areas. Finally, the intricate kinegram designs issued up to now can hardly be called schematic, so the above claim of superiority cannot be considered well founded. Furthermore, it appears that current pixelgrams also incorporate kinematic effects, although, in contrast with the line art of kinegrams, these are composed of the apparent movement of notably extended image surfaces. If nothing else, the pixelgram would probably penetrate the realm of the kinegram and violate proprietary affairs. From the standpoint of visual perception, as set forth in Chapter 9, Section 9.3.2, line art kinematic effects would be superior to the kinematic movement of extended image elements.

The pixelgram diffractive structure is manufactured by means of electron beam lithography. Each diffraction groove is written separately by a focused electron beam, scanning across an electron-sensitive resist layer. This technique renders structures with very fine submicroscopic detail. Because advanced electron beam lithographic technology allows perfect control of groove shape and period, pixelgrams can be fabri-

cated with near theoretical diffraction efficiency. Additionally, electron beam technology would allow the groove shape to be modeled to generate dissimilar plus and minus first orders (blazing), which offers protection against laser contact copying. However, this possible security application of electron beam lithography to the pixelgram has not yet been reported.

As mentioned, optical replication of pixelgrams appears quite possible. Pixelgram technology, however, is claimed to offer additional guard against laser contact copying, the copy becoming impaired by moiré fringes as a result of the "self-imaging" property of gratings [9,10]. This is called the *Talbot effect*, which manifests itself behind a grating, illuminated by a point source, in multiple images of that same grating at distances that are a function of the grating period and the wavelength [11]. As the distance between the original grating and the photosensitive layer unavoidably varies, the contact copy becomes covered with tiny moiré fringes. Usually this effect is only visible at considerable enlargement but, according to the inventor, the pixellated diffraction grating can be designed to show the moiré fringes on a macroscopic scale, which plainly exposes a contact copy in zero-order inspection. As of yet, this defense is a mere theoretical prospect, based on computer simulation of the expected effects and awaiting future realization.

Although no reports on machine inspection feasibility of pixelgrams exist, it should be clear that the pixel structure allows the addition of various types of machine-readable patterns. Like kinegrams, pixelgrams offer highly valuable security devices for first-line as well as machine inspection. Based on CAD technology, they present advanced pictorial designs. Contrary to the opinion of holographers, they are not to be ranked in the lower level of optical security devices. Nevertheless, pixelgram technology has not yet been applied commercially to security projects.

11.3.3 Zero-Order Diffractive Devices

Zero-order diffractive structures (ZODs) can be considered a transition between diffractive and interference structures (Chapter 10). The "nanosculpture" of matter culminates in this type of device, which confirms my position that security is associated with the structural complexity of matter. ZODs can be mass produced using conventional embossing technology and consist of intricate lamellar diffraction patterns with periods smaller than the wavelength of light, so that no visible first-order diffraction is produced. A main advantage of ZODs is that they allow inspection under any kind of illumination; whether completely diffuse or from a point source, whether under normal observation or at extremely steep angles, they display conspicuous and unique iridescent effects. In this respect, they are superior to any other iridescent device. In particular, this is an advancement over all first-order devices, which suffer a complete loss of diffraction effects under diffuse illumination.

A further advantage of ZODs over first-order devices is that their bright reflection does not depend on reflective metallic coatings but on the resonance of the

lightwaves with the lamellar structure. As a consequence, they can be applied as transparent overlays without any loss of reflectivity; even a purely white substrate is does not overpower the intensely colored zero-order reflection. This advantage ZODs share with all-dielectric thin film multilayers (Chapter 12) and Bragg structures, which also can be highly transparent while having a very high reflection efficiency in a limited spectral range (Sections 11.2.1 and 11.4). The difference, however, is that the reflection of the ZOD is highly anisotropic: its color changes on rotation in its own plane. In contrast, multilayers and Bragg structures are completely isotropic and show no color change on rotation in their own plane. This anisotropy is a very strong security feature and even though this color shift depends on lighting and observation conditions, it can be unambiguously defined (Chapter 10, Section 10.5.1).

The ZOD structure can be fully buried in a dielectric matrix, such as a plastic card, during the card lamination stage in stead of being applied to the card's surface in a late stage of the card production, like first-order devices. The ZOD structure is therefore well protected against attempts to uncover its structure for the purpose of mechanical replication. This latter characteristic it shares with well-manufactured first-order devices, which have their metallized microstructure embedded between chemically related plastic layers as well, to guard them against solvents that might lay the surface structure bare. This, combined with the fact that the unique optical characteristics of the lamellar structure cannot possibly be copied by optical means, makes the ZOD a security structure highly inaccessible to counterfeiting attempts.

A simple test with a polarizing sheet (polaroid sunglasses) will reveal the strong linear polarization of the light reflected by ZODs. ZOD structures show unique spectral and polarization characteristics that distinguish them from all other types of security structures and make them well suited for efficient machine inspection (Chapter 10).

Summarizing, ZODs offer forthright first-line security as well as machine inspection capabilities. In most aspects, their performance is superior to first-order devices. As yet, however, the ZOD technology awaits commercial application to security documents.

11.4 NONHOLOGRAPHIC MULTIPLE-LAYERED STRUCTURES

In all aspects, multilayered interference structures stand at right angles to diffractive structures (Chapter 3, Section 3.3.3). Whereas diffractive structures are "micro-carved" line by line into matter (for example, photoresist), interference structures are built up, layer by layer. Such "buildings" are another example of the intricate way that matter can be organized to render unique optical effects that can be applied to security devices. The optical effects generated must be sufficiently different from what can be achieved by holographic Bragg structures, as the latter are produced too easily in a moderately equipped laboratory

As zero order structures, multilayers have the potential to render highly transparent overlays, with an efficient reflection in a waveband that varies with the angle of observation. This is a notable advantage over first-order structures that can be rendered sufficient transparency only at a considerable expense of reflection efficiency.

Multilayers consist of a regular stack of thin films that reflect strong interference colors. They can either be thin film structures or Bragg structures. Thin film structures embody relatively few layers (three to a few tens) with a high difference of refractive index between the alternate layers, which consist of different materials. These can be all dielectric materials or combinations of metallic layers and dielectric layers (Chapter 12). Bragg structures incorporate many layers (tens to hundreds) with only a small difference of refractive index between them, generally brought about by small changes in concentration of a single dielectric material (Chapter 3, Section 3.3.3, and Chapter 13). Both types can acquire reflection efficiencies of the interference waveband of up to 100%. Evidently thin-film multilayers are more intricate than Bragg structures and thus can be expected to offer better security prospects.

Contrary to first-order diffractive structures, under diffuse lighting conditions, like an overcast sky, all multilayers, whether holographic or nonholographic, perform rather well, showing a persistent iridescence and well-defined colors. They have this in common with zero-order diffraction devices, although these perform well under all kinds of lighting.

In contrast with volume-reflection holograms (Section 11.2.1), a characteristic of nonholographic multilayers is their parallel alignment with the substrate, so that the interference colors reflected by these structures tend to coincide with the specular reflection of the structure. If multilayers are protected by laminating foils or laquers, this results in a disadvantageous overlap of the interference colors with the white specular reflection of the smooth protective layer. The interference colors reflected by well-configured multilayers, however, will exhibit a much higher luminous reflectance than the white specular reflection of the protective surface. Furthermore, if the multilayer structure has a microsurface roughness, the interference colors will also show outside the specular reflection of the smooth protective layer. Cholesteric liquid crystals exhibit a statistical angular fluctuation of their micro structure, which renders their interference colors a matte appearance, visible at angles far outside the specular reflection. The specular reflection of the protective surface tends to overpower the interference colors of liquid crystals.

Rather complex designs in multilayers are possible, like logos and alphanumerics, by such techniques as masking and laser ablation. The optically variable effects of multilayers are generally fairly modest compared to those of multiple gratings. More intricate, highly secure multicolor designs of multilayers are possible, in thin film as well as liquid crystals, but these are fairly expensive.

In general, the nonexpert will not easily distinguish between ordinary thin-film devices, pearl luster inks, and Bragg structures. This entails a certain security hazard because holographic Bragg-type or pearl luster imitations of ordinary thin-film and

structures to ensure an adequate distinction with such simulations. The more intricate the construction of the multilayer, the more security it will render. Mass production of multilayer structures, whether consisting of the thin film type or of polymerized liquid crystals, has been realized.

Machine readability of multilayers must be based on their spectral composition and polarization effects. The spectral composition is the only useful machine inspection parameter of the isotropic thin film structure, while anisotropic liquid crystals show circular polarization effects that add to their unambiguous machine inspection capability.

11.4.1 Thin Films

Thin film devices are composed of a stack of different layers that can be either all-dielectric or consist of alternating dielectric and metallic layers [12–16]. The latter type naturally is opaque but the all-dielectric type stacks are transparent and can show a spectral band reflection near 100% if the stack consists of a sufficient number of layers. The application of many layers, however, is expensive, so that in practice the number of layers tends to be confined to five. Examples are the British Columbia (Canada) driver's license, the Canadian $50, $100, and $1000 bills and optically variable ink.

British Columbia Driver's License

Although this limits the reflection efficiency, such a small number of layers can nevertheless be adequate to render a bright semitransparent security overlay of almost 50% luminous reflectance. For instance, the thin-film device for British Columbia's driver's license shows a bright golden specular reflection that flips to a transparent complementary bluish color outside specular reflection (Figures 12.5(a) and 12.6(a)). This structure performs very well: even on a white background, the specular reflection of the laminating foil does not overpower the bright golden interference color. For those who are used to the substantial color shift of Bragg structures with angle of observation, this particular thin film device shows a negligible color shift: the display remains golden only to attain a greenish yellow tone under acute angles of observation. As a result, the film is reminiscent of common hot stamping gold foil, from which it differs though by its obvious bluish transparency. Its high specular reflectance distinguishes it from the more diffuse shimmer of pearl luster pigments. The golden gloss is only visible in a rather narrow angle about the specular reflection, which makes its very bright but at the same time more difficult to find (see Appendix A).

Canadian Banknotes

In contrast, the thin-film device on the Canadian $50, $100, and $1000 denominations

angle of observation, which is reminiscent of Bragg reflection. The iridescent effect is visible in a relatively broad angle about the specular reflection due to the introduction of microcracks in the thin-film structure, which render it a matte reflectance (Chapter 12, Section 12.2.4). This specific matte iridescent gloss adequately distinguishes the device from regular holographic Bragg structures, while its substantial color shift distinguishes it from the virtually monochrome pearl luster pigments. It performs best under diffuse lighting and although all-dielectric, it is opaque because of the application of a black adhesive.

Optically Variable Ink

Metal dielectric thin films can be made into microflakes and added to a transparent ink medium to render an optically variable ink (OVI) [17–19]. Their large color shift with angle of observation distinguishes OVIs from common pearl luster inks. Such security inks are, for instance, applied on the German DM500 and DM1000.

Because the angular alignment of the flakes in the printed ink is somewhat random, the OVI print has a matte gloss and its color shift is visible under all lighting conditions, though the effect is not very conspicuous. Possible color changes of metal dielectric films are illustrated in Figure 12.4. The color of OVI can be completely derived from interference effects without additional pigments. OVI printing can be part of a graphical design printed in conventional inks so that under normal observation the two are indistinguishable and only become so under more acute angles of observation. The intricate production technique makes this ink a very expensive one, only reserved for security purposes.

11.4.2 Pearl Luster Inks

Pearl luster inks are sometimes classified as optically variable inks. Their lustrous shimmer is based on light interference in single high-refractive-index metal oxide layers on mica microflake carriers (Chapter 3, Section 3.3.2). The spectral reflection of a TiO_2 pearl luster pigment in a medium is only about 30% (Figure 3.7), but if well applied, its colored shimmer is sufficiently conspicuous even on a white background, while outside the specular reflection the background takes a slight complementary hue. The color shift with angle of observation is negligible. They can be used as security overlay printing over personal data in pouches and laminates as well as in security printing on paper. Agfa has introduced security printing with high-quality pearl luster pigments, showing very prominent effects (Chapter 17). An example is the golden pearl luster printing on the new Dutch hundred guilder note.

Because of their simple construction, these pearl luster pigments are inexpensive and their wide commercial availability might restrict their security value. Again, security seems to be associated with the structural complexity of matter.

11.4.3 Liquid Crystals

Like thin-film devices liquid crystals are multilayered structures (Chapter 13), but they are of the Bragg type and only consist of one substance, which shows slight alternate changes in refractive index (Chapter 3, Section 3.3.3). This is the type of structure that runs a certain risk of being imitated by holographic Bragg structures unless it consists of (expensive) multicolor designs. Liquid crystals, however, are distinguished from holographic structures by their strong polarization effects. Contrary to thin-film overlays, which tend to be very bright but have a strongly limited angular perceptibility, liquid crystal devices are considerably less bright but tend to be visible under wider angles. A further disadvantage of their reduced brightness is that they become less conspicuous against a white background. This limits their security value. Chapter 13, Section 13.3.2. treats possible machine inspection techniques.

11.5 DISCUSSION AND SUMMARY

Different security devices may be based on very different security conceptions and therefore cannot be compared without taking such conceptions into consideration. Unfortunately such undiscerning comparisons are frequently made.

Holographic security devices are based on their unique 3-D image capacity, in particular, that of human portraits. Their reproduction can be extremely difficult because of the elaborate recording techniques involved (Chapter 8, Section 8.3.2).

The designers of the pixelgram share the opinion of some holographers that the uniqueness of the human portrait comprises certain security advantages but wish to avoid the disadvantages of 3-D images under diffuse lighting.

The kinegram concept is based on well-defined movements and form changes, taking certain mnemonic aspects of visual perception into account (Chapter 9, Section 9.3.2). It has intentionally abandoned 3-D images.

All these devices share their pleasing first-order color variability, which, however, depends on the lighting conditions and is hard to define unambiguously. Furthermore, their reflectivity is based on the addition of a thin metal layer that makes them opaque and unfit as a security overlay. Although they can be rendered sufficient semitransparency by the choice of alternative reflective layers, this is at a notable expense of reflectivity.

This is where ZODs have a substantial advantage over first-order devices. They display very bright, well-defined, and unique variable color effects, almost entirely independent of lighting and observation conditions. Yet they are highly transparent outside the reflected waveband and thus render high-quality security overlays. The security concept of ZODs is not explicitly based on any specific theory of visual perception, and neither is that of multilayer structures like thin films and Bragg structures. Like ZODs, independent of lighting conditions, these can show a notable

color variability, but due to their laminar structure, unlike ZODs, they exhibit these colors under an only limited angle of observation. If all dielectric, they may yield bright and transparent security overlays.

REFERENCES

[1] Hopwood, A. I., "New Holographic Overlays," *SPIE Vol. 1509 Holographic Optical Security Systems*, The Hague, 14–15 March 1991, pp. 26–35.

[2] McGrew, S. P., "Hologram Counterfeiting, Problems and Solutions," *SPIE Vol. 1210 Optical Security and Anticounterfeiting Systems*, 15–16 January 1990, Los Angeles, California, pp. 66–76.

[3] McGrew, S. P., "Countermeasures against hologram counterfeiting," *Optical Security Systems, International Symposium and Product Presentation for Optical Information Storage and Display*, Zurich, Switzerland, October 14–16, 1987.

[4] Antes, G., "Dokument mit einem beugungsoptischen Sicherheitselement," Landis & Gyr Zug AG, Zug, Switzerland, *patent number EP 0 105 099*, April 4, 1984 (priority October 4, 1982).

[5] Iwata, F., and Kazuhiko, O., "Grating Images," *Proceedings 2nd International Symposium for the Application of Holography in Security, Optical Data Storage and Display*, Zürich, October 12–14, 1988.

[6] Longhurst, R. S., *Geometrical and Physical Optics*, Chapter XII, "Diffraction Gratings," London: Longmans, Green and Company, Ltd., 1957.

[7] Schuurman, D., "Fraud involving OVDs and possible security measures," *SPIE Vol. 1509 Holographic Optical Security Systems*, The Hague, 14–15 March 1991, pp. 126–130.

[8] Lee, R. A., Jackson, W. K., and Goodman, R. A., "Diffraction grating," Reserve Bank of Australia, Martin Place, Sydney, NSW 2000 (AU), *patent number WO90/07133*, June 28, 1990.

[9] Lee, R. A., "Diffraction grating and method of manufacture," Commonwealth Scientific and Industrial Research Organization, Limestone Avenue, Campbell, ACT 2601 (AU), *patent number WO91/03747*, March, 21, 1991.

[10] Lee, R. A., "The Pixelgram–An application of electron beam lithography for the security printing industry," *SPIE Vol. 1509 Holographic Optical Security Systems*, The Hague, 14–15 March 1991, pp. 48–54.

[11] Edgar, R. F., "The Fresnel diffraction images of periodic structures," *Optica Acta*, Vol. 16, No. 3, 1969, pp. 281–287.

[12] Berning, P. H., Phillips, R. W., "Thin film optically variable article having substantial color shift with angle and method," Flex Products, Inc., Santa Rosa, Calif., *patent number EP 0 170 439*, February 5, 1986.

[13] Phillips, R. W., Spellman, V. C., Gossett, W. L., Kamerling, M. A., "Tamper evident optically variable device and article utilizing the same," Optical Coating Laboratory, Inc, Santa Rosa, Calif., *patent number U.S. 4,721,217*, January 26, 1988.

[14] Phillips, R. W., Willison, C. R., "Preimaged high-resolution hot stamp transfer foil, article and method," Flex Products Inc., Santa Rosa, Calif., *patent number EP 0 341 047*, November 8,

[15] Berning, P. H., Phillips, R. W., "Thin film optically variable article and method having gold to green color shift for currency authentication," Flex Products Inc., Santa Rosa, Calif., *patent number U.S. 4,930,866*, June 5, 1990.

[16] Phillips, R. W., Coombs, P. G., "Transparent Optically Variable Device," Flex Products Inc., Santa Rosa, Calif., *patent number EP 0 395 410*, October 31, 1990.

[17] Phillips, R. W., Mayer, T., Ash, G. S., "Optical thin film flakes, replicated optical coatings and inks incorporating the same and method," Flex Products, Inc., Santa Rosa, Calif., *patent number EP 0 227 423*, July 1, 1987.

[18] Ash, G. S., "Article and method for forming thin film flakes and coatings," Optical Coating Laboratory, Inc., Santa Rosa, Calif., *patent number U.S. 4,434,010*, February 28, 1984.

[19] Gray, H. R., Shimshock, R. P., Krisl, M. E., "Method for making pigment flakes," Deposition Sciences, Inc., Santa Rosa, Calif., *patent number U.S. 4,879,140*, 7 November 1989.